Program Cyber Security Plan
Exhibit 4 – Unclassified Information Systems

1.0 Purpose

The purpose of this document is to provide the Office of Science (SC) a direction on a consistent method to implement cyber security in a manner that ensures the security of information and information systems of all Federal and contractor staff while meeting mission requirements. In addition, the PCSP will aid in the implementation of the federally mandated Certification and Accreditation (C&A) in SC for unclassified information systems.

2.0 Responsibilities

The roles and responsibilities for implementing this document are described in the Office of Science Program Cyber Security Plan (PCSP).

3.0 PCSP Operation

3.1 Overview

The Office of Science (SC) implements cyber security activities to protect its information and information systems utilizing the principles and functions of NIST to secure unclassified information systems. SC staff: 1) ensure that applicable implementation guidance is followed by SC staff; 2) ensure that appropriate cyber security implementation guidance is placed into contracts; 3) provide oversight of contractor OCIO policies and guidance cyber security work planning and controls; 4) integrate continuous feedback and improvement mechanisms into their work; and 5) perform the necessary oversight /assessments of both the Federal staff and contractors.

The PCSP addresses the requirements for SC staff in the relevant aspects of cyber security and performance of OCIO policies and guidance that are Federal responsibilities. Furthermore, the PCSP serves to ensure that OCIO policies, guidances, and methods of accomplishment are identified, communicated, and implemented by both Federal staff and contractors. This includes the oversight, assessment, and evaluation of both Federal staff and contractor performance, and reporting of cyber security performance data to SC and other entities (e.g., U.S. Department of Energy and, as appropriate, Federal, state, and local governments). Effective implementation of the PCSP will ensure the security of information and information systems of SC staff.

The processes for addressing contractor PCSP performance expectations are outlined in the respective Cyber Security Program Plans (CSPP) of the SC laboratories and site offices.

3.2 Key Functions/Services and Processes

3.2.1 PCSP Subject Areas for Functions/Services and Processes for Federal Staff

SC PCSP requirements, responsibilities, and authorities for the Federal staff are included in the DOE Order 205.1A, "*Department Of Energy Cyber Security Management*". The Cyber Security Management (CSM) structure establishes a program whereby the staff plans, performs, assesses, and improves the security of information and information systems within the Department of Energy (DOE). This program is institutionalized within SC at Headquarters, the Integrated Service Centers, Site Offices and Laboratories, with the development of Cyber Security Program Plans (CSPP) for unclassified systems. The following sections describe the SC direction issued by the OCIO to ensure compliance with PCSP requirements. The following subsections are the corresponding PCSP implementation ensuring direction is aligned with SC's mission.

3.2.1.1 Process for Assessing Risk and Securing Cyber Systems

The Office of Science is committed to ensure that all information systems are protected in accordance with the magnitude of harm that would occur should the information or the information system be compromised or destroyed. Cost effective cyber security is the goal of the SC unclassified information system cyber security program. This task describes the process by which all the information and information systems are evaluated for risk impact and grouped into accreditation boundaries (also known as enclaves) which are protected by various security controls. This task also includes the process by which artifacts are developed or updated; management, operational, and technical controls are identified; the controls are tested, and an authority to operate is issued. Section 5.1 contains an overview of this process.

3.2.1.2 Cyber Security Direction for Unclassified Systems

The Office of Science is committed to ensuring that the Federal staff performs required Federal program responsibilities in a cost-effective and efficient manner. SC organizations are expected to implement DOE OCIO policy and direction within a security framework applicable to their mission. SC ensures that Federal and contractor staffs are implementing their PCSP requirements and responsibilities by providing direction on OCIO Cyber Security Technical & Management Requirements (TMRs). This subject area (Section 5.2) identifies the security expectations for compliance with DOE cyber security direction.

3.2.1.3 Cyber Security Risk Mitigation Strategies for Unclassified Systems

SC is committed to providing specific direction on risk analysis to assure that mission requirements are satisfied without compromising the security of the Office of Science or DOE. Special guidance on some high risk areas is required due to their sensitivity. For example, the protection of Personally Identifiable Information (PII) has become an especially visible issue, and therefore SC has developed a policy for the protection of this category of information. This subject area (see Section 5.3) identifies the risk areas that require specific mitigation strategies.

4.0 Requirements

The following summarizes high-level requirements relevant to the PCSP.

P.L. 103-356, Government Management Reform Act of 1994, (October 13, 1994)

P.L. 104-208, Title VIII, Federal Financial Management Improvement Act of 1996 (FFMIA), (October 1, 1996).

P.L. 104-231, Electronic Freedom of Information Act (e-FOIA), (October 2,1996)

P.L. 107-347, Title III, Federal Information Security Management Act of 2002 (FISMA), (December 17, 2002)

P.L. 93-579, Privacy Act of 1974, as amended [Title 5 United States Code (U.S.C.) Section 552a], (December 31, 1974)

P.L. 96-349, Trade Secrets Act - (18 U.S.C., section 1905), (January 22, 2002)

P.L. 97-255, Federal Managers' Financial Integrity Act of 1982 (FMFIA), (September, 8, 1982)

P.L. 99-474, Computer Fraud and Abuse Act (18 U.S.C. section 1030), (October 16, 1986)

P.L. 99-508, Electronic Communications Privacy Act of 1986, (October 21, 1986)

P.L. 100-235, Computer Security Act of 1987, (January 8, 1988)

P.L.104-106, Division E, Clinger-Cohen Act (Information Technology Management Reform Act of 1996), (February 10, 1996)

OMB Circular A-123, Management Accountability and Control, (August 4, 1986), (revised Dec 21, 2004)

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-99-05, Instructions for Complying With The President's Memorandum of May 14, 1998, “Privacy and Personal Information in Federal Records”, (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)

OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, (December 20, 2000)

OMB Memorandum M-01-08, Guidance On Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and “File Sharing” Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments, (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, National Institute of Standards and Technology (NIST)[1] Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication[1] (SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling, (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006 (updated April 20, 2006)

NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

[1] Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-61, Computer Security Incident Handling Guide, (January 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, (July 2003)

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, (October 2003)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, (August 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE P 205.1, Departmental Cyber Security Management Policy, (May 8, 2001)

DOE O 205.1A, Department of Energy Cyber Security Management Program, (December 4, 2006)

DOE 0 221.2, Cooperation with the Office of Inspector General, (March 22, 2001)

DOE P 226.1, Department of Energy Oversight Policy, (June 10, 2005)

DOE 0 226.1, Implementation of Department of Energy Oversight Policy, (September 15, 2005)

DOE P 470.1, Integrated Safeguards and Security Management (ISSM) Policy, (May 8, 2001)

DOE 0 470.2B, Independent Oversight and Performance Assurance Program, (October 31, 2002)

DOE 0 471.1, Identification and Protection of Unclassified Controlled Nuclear Information, (June 30, 2000)

DOE 0 470.4, Safeguards and Security Program, (August 26, 2005)

DOE 0 475.1, Counterintelligence Program, (February 10, 2004)

E.O. 12344, Naval Nuclear Propulsion Program, (February 1, 1982)

E.O. 12958, Classified National Security Information, (April 17, 1995)

E.O. 13011, Federal Information Technology, (July 17, 1996)

E.O. 13231, Critical Infrastructure Protection in the Information Age, (October 16, 2001)

E.O. 13228, Establishing the Office of Homeland Security and the Homeland Security Council, (October 8, 2001)

Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, (December 17, 2003)

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors, (August 27, 2004)

5.0 Subject Areas

5.1 Process for Assessing Risk and Securing Cyber Systems

The Office of Science follows the FISMA implementation project model to assess risk and secure information systems. The process is illustrated in Figure 5.1. The approach is comprised of those activities that are specifically required within the FISMA framework and detailed in statutorily required NIST standards and guidance. As illustrated in Figure

5.1, below, these activities are part of a cyclical continuous improvement process, and the conclusion of one cycle starts the next iteration.

Prior to the analysis, system data is collected. This information describes the purpose of the information systems, who owns the systems, what data is collected and their physical location of the servers, and end user devices. Based upon the information collected from existing documentation and interviews with system owners; the sensitivity of information contained in each system is determined and an initial impact rating of systems is generated. Systems are ranked as high, moderate, or low with respect to impact from loss or compromise of data.

Systems with the same risk impacts can be grouped together – assuming they are under the same management control. Most (if not all) SC systems are expected to be evaluated as either low or moderate risk impact

This grouping of systems is used to select an appropriate set of security controls. The controls implemented must be cost effective to the organization. The entirety of this effort is documented in the CSPP. A set of the NIST compliant cyber security documents are generated which includes a threat statement, risk assessment, CSPP, supplementary controls, etc.

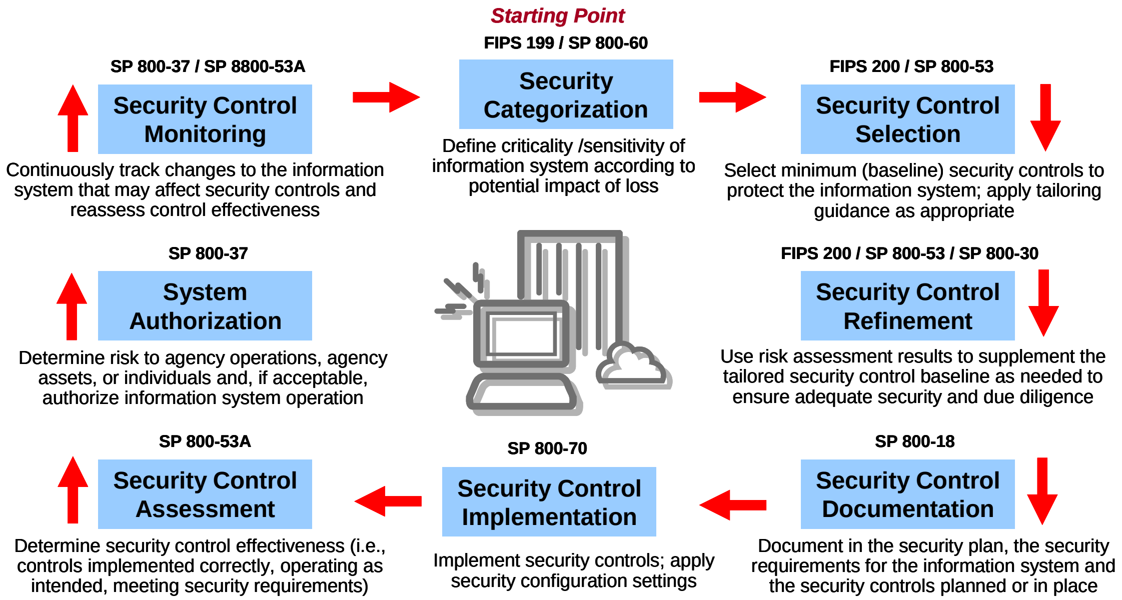
Starting Point
FIPS 199 / SP 800-60
Security Categorization
Define criticality /sensitivity of information system according to potential impact of loss
FIPS 200 / SP 800-53
Security Control Selection
Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate
FIPS 200 / SP 800-53 / SP 800-30
Security Control Refinement
Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence
SP 800-18
Security Control Documentation
Document in the security plan, the security requirements for the information system and the security controls planned or in place
SP 800-70
Security Control Implementation
Implement security controls; apply security configuration settings
SP 800-53A
Security Control Assessment
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)
SP 800-37
System Authorization
Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation
SP 800-37 / SP 8800-53A
Security Control Monitoring
Continuously track changes to the information system that may affect security controls and reassess control effectiveness

Figure 5.1 FISMA Implementation Project Model

After the controls have been selected and implemented, the controls are tested to ensure that everything is functioning as specified. This requires the development of an independent Security, Test and Evaluation (ST&E) plan. The results of the ST&E are documented and, along with all the previous documents, are then compiled and provided to the DAA to obtain the Authority to Operate.

This last phase provides the DAA with the evidence required to ensure that SC management and staff are made aware of the threats, vulnerabilities and risks; and that the management, operational, and technical controls are in place and working. The DAA can then make a rational decision concerning whether or not the system is allowed to operate under these conditions. The DAA is accountable to assure that the agreed upon controls continue to operate as specified throughout the life cycle of the system, or that the operational environment is re-assessed if a significant change to the environment is made.

5.2 Cyber Security Direction for Unclassified Systems

Below is SC's analysis and direction on each of the OCIO Cyber Security (CS) guidance documents[2]. SC complies with statutory requirements, OMB requirements, NIST, FIPS requirements, and Departmental policy. The SC cyber security program is centered on the NIST SP 800 series and OMB guidance. Each site should review the guidance documents to assure that controls being implemented are consistent with this section. This section will evolve as new OCIO CS Guidance and Technical and Management Requirement (TMR) documents are issued.

The CS numbers correspond to the OCIO's numbering schema and not all numbers are sequentially addressed.

CS-01, Management, Operational, and Technical Controls Guidance

- Analysis -- The document identifies the management, operational, and technical controls necessary to safeguard information systems rated as high, moderate, or low. Although it is consistent with the original version of NIST SP 800-53, "*Recommended Security Controls for Federal Information Systems*", it is not consistent with latest version of that NIST document (Revision 1-December 2006).

  A Security Test and Evaluation is conducted on the controls to determine if they perform as intended and provide the functionality required of the control. SC supports all the controls in NIST 800-53 (Revision 1) and, in many cases, the implementation of the control is to a more restrictive measure than what is defined in CS-01.

- SC Direction -- Implement the newest version of NIST SP 800-53 (Revision 1) with consideration of the guidance in CS-01. Periodicity of control implementation and how the site or facility will satisfy that control will be documented in the CSPP. The DAA will make the final decision as to the effectiveness of the controls, and when satisfied that the system is operating at an acceptable risk level, issues an Authority to Operate

[2] SC PCSP direction will reflect CIO Cyber Security Guidance until the OCIO Cyber Security Cyber Security Technical and Management Requirements are issued. Updates to OCIO cyber security guidance are shown on http://cio.energy.gov/policy-guidance/guidance.htm.

CS-02, Certification and Accreditation Guide

- Analysis -- The document outlines the Certification and Accreditation process. It is generally consistent with the NIST SP 800-37, "*Guide for the Security Certification and Accreditation of Federal Information Systems*".

- SC Direction -- Implement the newest version of NIST SP 800-37 with consideration of the guidance in CS-02. The DAA will make the final decision as to the effectiveness of the controls, and when satisfied that the system is operating at an acceptable risk level, issues an Authority to Operate

CS-03, Risk Management Guide

- Analysis -- The document identifies the process of analyzing cyber security risks and is consistent with NIST SP 800-30, "*Risk Management Guide for Information Technology Systems*". There is a requirement to use the DOE threat statement as a baseline for the analysis. There is also a requirement to have systems tested and evaluated – SC interprets this to be security test and evaluation.

- SC Direction -- Risk management is pivotal to the implementation of effective cyber security. SC will implement NIST, FIPS 199, NIST FIPS-200, and NIST SP 800-30 with consideration of the guidance in CS-03. Risk is assessed at the site and enclave level. The threat statements must be customized to reflect each site's environment and are currently based on a SC-wide threat statement that reflects the most common vulnerabilities with unclassified information systems. The DOE threat statement will also be used when it is issued

CS-04, Vulnerability Management Guide

- Analysis -- The document identifies requirements for vulnerability scanning and patching, and is consistent with NIST SP 800-40, "*Creating a Patch and Vulnerability Management Program"* and NIST SP 800-42, "*Guideline on Network Security Testing*". The guidance document states that a risk based approach should be used to determine scanning frequency and that a maximum test period should be established.

- SC Direction -- The SC policy is to implement the NIST SP 800-40 and 42 with consideration of the guidance in CS-04. Scanning should be continuous, though the level of scans may differ depending on mission requirements. Patch management must be deployed with a periodicity consistent with the sensitivity of the information and information system being protected. In some cases, this may require that a patch be installed within a 24 hour period if the vulnerability is considered high. During ongoing research, the patching of some systems may be scheduled to coincide with the operating period of an experiment. Periodicity will be documented in the CSPP.

CS-05, Interconnection Agreement Guidance

- Analysis -- The document identifies requirements, processes, and procedures for planning, documenting, and managing system interconnections; and is consistent with NIST SP 800-47, "*Security Guide for Interconnecting Information Technology Systems*". The guidance document requires that the specific hardware and configuration of the connecting systems be identified.

- SC Direction -- This document is being implemented through NIST SP 800-47 and the SC policy shown in Section 5.3. The guidance document is focused on the level of security (low, moderate, high) that is being enforced, regardless of the specific hardware configuration of the systems. The Memorandum of Understanding (MOU) document in Section 5.3 is consistent with CS-05.

CS-06, Plan of Actions and Milestones (POA&M) Guidance

- Analysis -- The document identifies the requirements for developing, documenting, and implementing a Plan of Actions and Milestones process and is consistent NIST SP 800-37. The document requires POA&M items that have been verified and closed to continue to be reported for at least a year. The document also requires the reporting of "no POA&M" items.

- SC Direction -- SC policy is to implement NIST SP 800-37 and consider the guidance in CS-06. However, there will be no POA&M items resulting from the initial on-site portion of a site visit of a SC element for one year. After that period, all items must be reported and tracked through the POA&M process. The site visit leads to enhancement of the cyber security program, implementation of the controls, and upgraded documentation. This results in a NIST compliant certification and accreditation package for the systems with an accompanying POA&M

CS-07, Contingency Planning Guidance

- Analysis -- The document identifies contingency planning responsibilities and requirements and is consistent with NIST SP 800-34, "*Contingency Planning Guide for Information Technology Systems*", and there is general agreement on the purpose and process for establishing a contingency plan. The guidance document requires that contingency plans be developed for Critical Infrastructure or Key Resources, and that contingency plans tests are either functional tests or table-top exercises.

- SC Direction -- SC will implement NIST SP 800-34 with consideration of the supplemental guidance in CS-07. Additionally, SC will implement contingency plans through the CSPP level. There are some SC facilities which may have limited contingency plans or plans that are less detailed than described in this document. This is typically because the business impact analysis either permits a 5 day restoration period, which can be accomplished with vendor provided equipment, or because backup for the system is not practical. For example, one of a kind experimental or computation facilities, if destroyed, may not be repaired but may be replaced by the next generation of facility or item, or DOE may decide this capability will not be replaced. SC does not have any systems that are considered Critical Infrastructure or Key Resources as defined in HSPD-7. SC considers on the job training or replacing key equipment from an information system as a valid substitute for a Contingency Plan test.

CS 08, Configuration Management Guidance

- Analysis -- This guidance document is in concert with best practice for computer security configuration. The requirement is that network devices should support a national minimum security configuration setting. These national setting are determined by Center for Internet Security (CIS) National Security Agency (NSA), or Defense Information Systems Agency (DISA).

- SC Direction -- SC will implement standardized CIS level 1 settings for workstations and networked devices. Changes to the standard settings must be documented in the CSPP and accounted for in the risk assessment. Technically, all sites must have notification software that detects unauthorized changes automatically so that these changes can be flagged for the system administrator.

CS-09, Incident Management Guidance

- Analysis -- The document contains policy on reporting of cyber security incidents. The guidance contains basically the same text as the DOE Manual 205.1-1, *"Incident Prevention, Warning and response (IPWAR)"*. The requirements have been enhanced to include loss, theft and missing laptops/IT resources; and improperly purged or sanitized media. There are new reporting requirements for each incident that includes an impact assessment for each incident. Responsibilities for completion of these requirements will be defined in the CSPP SSP.

- SC Direction -- SC policy is to implement the DOE Manual 205.1-1 with consideration of the guidance in CS-09. There are new reporting requirements for each incident that includes an impact assessment for each incident. Responsibilities for completion of these requirements will be defined in the CSPP. Impact assessments will be sent to the SIO for review and comment.

CS-11, Media Clearing, Purging and Destruction Guidance

- Analysis -- The document provides policy on the cleaning destruction and reuse of media. IT has requirements beyond the existing DOE Manual 205.1-2, "*Clearing, Sanitization and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual"*. It is prescriptive in the treatment of media reuse and covers substantially more media products that the legacy DOE manual. This document allows media to be returned to vendor if the information on the media is low risk. The policy allows SC to outsource the purging/clearing of media to another

DOE facility/agency or authorized contractor. Handling of thumbdrives with sensitive but unclassified information will need to be addressed in the CSPP.

- SC Direction -- SC policy is to implement the DOE Manual 205.1-2 with consideration of CS-11.

CS-12, Password Management Guidance

- Analysis -- The document provides policy on password structure and guidance to the DOE M 471.3-1, "*Manual for Identifying and Protecting Official Use Only Information*". It is consistent with NIST SP 800-59 and there is general agreement on the purpose and process for establishing passwords. The guidance allows for passwords based on entropy which currently cannot be checked for compliance via existing software tools.

- SC Direction -- SC policy is to implement the DOE M 471.3-1, "*Manual for Identifying and Protecting Official Use Only Information*" with consideration of the guidance in CS-12. SC will only allow passwords that can be checked for rigor with a software tool to test the strength of the password. This means that entropy based passwords are currently excluded. SC supports password change a minimum of every six months or immediately if the password is suspected of compromise.

CS-13, Wireless Devices and Information systems Guidance

- Analysis -- The document provides policy on the use of wireless devices. It is consistent with NIST SP 800-48, "*Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*" and there is general agreement on the purpose and process for implementation of wireless networks. The document includes prohibitions on downloading freeware/shareware using wireless.

  The NIST document on wireless (SP 800-48) is relatively out of date, and some of the concerns with wireless communication have been resolved with newer standards. If the newer encryption standards are enforced, wireless networking can be used with wired networks. The document also requires an isolated C&A package solely for wireless systems. SC's policy is that if accreditation boundaries contain wireless devices, then specific controls should be in place to protect information over the wireless segments and therefore a separate C&A package is not required. SC will implement wireless security through the CSPPs. Wireless enclaves typically must be isolated in public enclaves and at least Wired Equivalent Privacy (WEP) encryption must be enabled. If the wireless enclave is connected to a wired enclave, then Wi-Fi Protected Access (WPA) encryption must be implemented. The enclaves that include wireless devices will have controls tested in the ST&E plan for that enclave as part of the C&A process.

- SC Direction -- SC policy is to implement NIST SP 800-48 with consideration of CS-13. Wireless is typically a separate enclave in SC but may, in some cases be combined with larger enclaves.

CS-14, Portable/Mobile Devices Guidance

- Analysis -- The guidance has been broadened to include personal laptops, PDA/Blackberries, cell phones, MP3 players, and other devices that collect/transmit/store DOE information. The policy requires that portable/mobile devices used to process DOE information, taken outside the United States be, at a minimum, sealed with a tamper indicating device or subject to a hardware/software technical review process upon leaving and re-entering the United States.

  Key to implementing this document is minimizing DOE information on portable devices, especially those traveling outside the United States. Currently, each facility or site will document how they meet the requirements in their CSPP. Ultimately, SC will be required to develop program-wide management/operational or technical controls to meet this requirement, to compensate for complete hardware/software technical reviews for equipment leaving the United States.

- SC Direction -- SC policy is to consider the guidance in CS-14. Specific direction on Personal Digital Assistants (PDA) is discussed in Section 5.3.

CS-15, Personally Owned Devices Guidance

- Analysis -- The guidance states that the Program Cyber Security Plan (PCSP) and supporting documentation should have defined policies and procedures for the use of personally owned devices (as opposed to government or contractor provided devices) that are used within the DOE facilities. Specific concerns are the use of devices in secure areas, a well as devices which may contain Sensitive Unclassified Information (SUI). SC is evaluating the implementation of Pointsec PC (a type of encryption software) to provide protection of information stored on fixed media, such as a desktop or laptop.

- SC Direction -- SC policy requires the same level of controls for personally owned devices that it does for government or contractor devices. All devices that connect to a DOE information system must be scanned, registered in the site network, and required to have a current anti-virus application installed with all updated security patches applied to the operating system. SC policy is to consider additional guidance in CS-15.

CS-18, Foreign National Access to DOE Information Systems Guidance

- Analysis -- The guidance is consistent with DOE O 142.3, "*Unclassified Foreign Visits and Assignment Program*" for unclassified systems in that it recognizes background checks should be dependent on the level of access granted (general user, privileged user and administrator) and type of information being accessed. SC has developed an access policy consistent with this approach.

- SC Direction -- SC policy is based on the role of an individual and their trustworthiness rather than on their place of birth. Although DOE O 142.3, "*Unclassified Foreign Visits and Assignment Program*" must be implemented, SC policy on access is discussed in Section 5.3.

SC-20, Information Condition (INFOCON) Guidance

- Analysis -- The document establishes an overall graded approach to cyber security escalation and actions similar to the Department of Homeland Security (five color levels). The incident reporting process describes actions to be taken in the event of a compromise or suspected compromise and they are consistent with the guide.

  SC Direction -- SC has procedures in place to respond to external threats. Incident procedures, as well as the normal control in place for information security result in a posture consistent with "code yellow." Each site has the capability to shut off specific ports, applications, or processes in the event of a suspected attack, or to facilitate forensic analysis. The INFOCON process is part of overall incident reporting/alert procedures and is managed centrally by the DOE's Chief Information Officer. SC policy is to take CS-20 under consideration.

CS-23, Peer to Peer Networking (P2P) Guidance

- Analysis -- The document is concerned with the legal and ethical security aspects of P2P networking. SC agrees that information systems that contain Personally Identifiable Information should not be in a P2P configuration. SC also agrees that the decision to incorporate P2P communication should be left to senior management. SC interprets required by P2P access controls that reflect the information types and security category of the system to relate to national security system controls is therefore not applicable to unclassified systems.

- SC Direction -- SC will allow P2P networking at the discretion of senior management for the purpose of sharing research information. Accreditation boundaries that include P2P systems will have controls in place for the identification of system use, files accessed, users, time of day and other common logging and identification controls enforced as part of a defense in depth. Controls must be documented in the CSPP.

CS-24, Remote Access Guidance

- Analysis -- This guidance identifies measures related to accessing DOE and contractor information systems from outside of the enclave or accreditation boundary.

Implementation of the controls in NIST 800-53, "*Recommended Security Controls for Federal Information Systems*" with consideration of the guidance in CS-24 is an access control issue.

- SC Direction -- SC policy on remote access is governed through the interconnection agreement as discussed in Section 5.3. Consideration will be given to the guidance in CS-24. Additional, SC policy is to implement the controls in NIST 800-53 that are documented in the CSPP. Furthermore, users are allowed access to information systems based on the role of an individual and their trustworthiness as discussed in SC policy on CS-18 and Section 5.3.

CS-37, Security Testing Guidance

- Analysis -- This guidance for implementing a Security, Test and Evaluation (ST&E) as part of the C&A process for unclassified systems aligns with NIST SP 800-37.

- SC Direction -- SC policy is to implement NIST SP 800-37 with the consideration of the guidance in CS-37.

CS-38A, Protection of Sensitive Unclassified Information including Personally Identifiable Information Guidance

- Analysis -- This document aligns with new the OMB direction for handling Personally Identifiable Information. All mobile/portable devices are assumed to contain Personally Identifiable Information or Sensitive Unclassified Information and must be protected in accordance with a NIST FIPS 140-2 compliant encryption. Exceptions to this policy are to be documented in the PCSP

- SC Direction -- SC policy is to implement SC requirements in Section 5.3. Section 5.3 contains additional guidance on the handling of Personally Identifiable Information. Consider the guidance in CS-38A.

5.3 Cyber Security Risk Mitigation Strategies for Unclassified Systems

The following section contains specific direction on risk analysis to assure that mission requirements are satisfied without compromising the security of the Office of Science.

5.3.1 SC Policy on CS-18, Foreign National Access to DOE Information Systems

All access to SC computing systems will be determined by the type of system to which the access is requested. Science has three major types of systems as indicated below. Access is granted consistent with programmatic needs, and subject to a risk assessment. Each laboratory must maintain a list of systems that fall into Type 2 and 3.

Type 1: Scientific Research Systems

These systems are for the purposes of scientific research and in general have no specific security restrictions. Moreover, remote access to these systems by scientists worldwide is important for scientific collaboration.

The following personnel screening controls are required for users who have access to this class of information systems. For **local users**, **local administrators** and **system administrators**, a Human Resource (HR) background check is required for access by all employees.[3]

Type 2: Infrastructure Systems

These systems are used to manage the "business end" of the laboratories. These systems include: payroll; travel; human resources; finance; and contracts. Many of these systems contain Personally Identifiable Information and because of the additional risks involved in this type of access, any individual granted access must be formally approved by a process that includes consideration of such factors as place of birth and citizenship, as well as level of experience, judgment, training, and other factors. All individuals granted access after this process must be approved by the appropriate authority.

The following screening controls are required for users who have access to this class of information systems. For **local users, local administrators** and **system administrators,** a Human Resource (HR) background check is conducted. For **domain administrators,** a National Agency Check with Inquiries must be conducted.

Type 3: Controlled Information Systems

Certain computer systems or information contain process or export controlled information, Unclassified Controlled Nuclear Information (UCNI) data, etc. Access to such systems can only be granted to in a manner consistent with the DOE policy.

The following screening controls are required for users who have access to this class of information systems:

- For **local users**, a Human Resource background check is conducted. If the user is given access to a controlled information system, a National Agency Check with Law and Credit (NACLC) and a Moderate Background Investigation (MBI) is required.

[3] There are four types of users discussed in the approach including:
- Local user – no ability to change configuration setting of the user workstation.
- Local Administrator – has ability to change the configuration settings of the user workstation.
- System Administrator - has ability to change the configuration settings of multiple workstations within the LAN segment.
- Domain Administrator – has the ability to configure network routers and gateways.

- For **local administrators**, at a minimum, a National Agency Check with Inquiries (NACI) is conducted. If the user is given access to controlled information, a National Agency Check with Law and Credit (NACLC) and a Moderate Background Investigation (MBI) is also required.

- For **system administrators**, prior to access approval, at a minimum, a background investigation (BI) and National Agency Check with Inquiries (NACI) is conducted. If the user is given access to a controlled information system, a National Agency Check with Law and Credit (NACLC) and an Extensive Background Investigation (EBI) is required.

For purposes of these designations, the following definitions apply:

- Human Resource (HR) Background Check: Confirms employment dates, job function, and education.

- National Agency Check (NAC): Part of every National Agency Check with Inquiries (NACI). Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), Federal Bureau of Investigations (FBI) Name Check, and FBI National Criminal History Fingerprint Check.

- National Agency Check with Inquiries (NACI): The basic and minimum investigation required for all new Federal employees consist of a National Agency Check (NAC) with written inquiries and searches of records. These cover specific areas of an individual's background during the past 5 years (with inquiries sent to current and former employers, schools attended, references and local law authorities). Coverage includes:

  Employment – 5 years
  Education – 5 years and highest degree verified
  Residence – 3 years
  Law Enforcement – 5 years
  National Agency Check (NAC)

- National Agency Check with Law and Credit (NACLC): Basic National Agency Checks (Security/Suitability Investigations Index, Defense Clearance and Investigations Index, fingerprint classification, and a search of the Federal Bureau of Investigation's investigative index). Credit search covering all residence, employment, and education locations during the last 7 years. Law Checks covering all locations of residence, employment, education during the last 5 year, admitted arrest, confirms identity, credit history, legal history and reason for access.

- Moderate Background Investigation (MBI): For example, a National Agency Check with Law and Credit (NACLC); contacts are made to neighbors.

- Background Investigation (BI): Contact neighbors and former colleagues to confirm lifestyle, allegiance to country, loyalty; usually goes back 5 years.

- Extensive Background Investigation (EBI): Same as above; goes back 15 years.

5.1.3.2 SC Policy on CS-14, Portable/Mobile Devices Guidance

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity and lower installation costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as PDAs (BlackBerry, CE windows devices, Palm Pilot, etc.) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail and Internet access. Here are the security requirements for BlackBerrys:

1) Users must set a BlackBerry device password.

Minimum Length - Your password must be at least 9 characters (9 characters are recommended because special characters, which increase the complexity of the password, cannot be used).

Password Pattern - It is recommended that you use combinations of alpha, upper/lower and numbers.

Security Timeout - When your BlackBerry is idle for more than 30 minutes, it is assumed to be in your holster and locked. You will need to enter your password to unlock your BlackBerry.

Password Age - Your BlackBerry password will expire after 180 days. You are notified on the day it expires and will be able to change it then. However, you can change your password at any time.

Set Maximum Password Attempts - After 10 failed attempts to enter a password correctly to unlock the BlackBerry, the device will automatically disable itself **and purge ALL DATA contained in the device.**

Maximum Password History - This prevents users from consecutively reusing the same password. Passwords may not be repeated until at least three different passwords have been used.

Forbidden Passwords - BlackBerry settings will not allow you to use ‘pass’ or ‘password’ as your password (or combinations of this, like p@ssw0rd) or any sequence of characters that is “easily guessed”.

Use the "lock" icon to lock your device.

2) Users must encrypt all data stored on BlackBerry devices. Data traveling to and from the BlackBerry is encrypted in transit. BlackBerry content settings will be established for each user to encrypt data on the device.

3) Users must immediately report a lost, stolen, or damaged device. If your BlackBerry is lost, stolen or damaged - contact your designated cyber representative immediately. The device can be disabled remotely, clearing all of the stored content in the process. Users should perform a full backup of all BlackBerry data prior to going on foreign travel in the event that a BlackBerry device is lost, stolen or confiscated by a foreign government. The help desk can provide assistance in performing this task.

5.1.3.3 SC Policy on CS-38A, Protection of Sensitive Unclassified Information including Personally Identifiable Information

The Office of Science (SC) protection policy for Personally Identifiable Information (PII) is consistent with DOE CIO-Guidance CS-38A.

Definition of Personally Identifiable Information

PII: Any information about an individual maintained by an agency, including but not limited to: education, financial transactions, medical history, criminal or employment history, and information which can be used to distinguish or trace an individual’s identity, such as their name, social security numbers, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Classes of Personally Identifiable Information

SC has identified two types of PII as follows:

- **Public Personally Identifiable Information**

  PII is available in public sources such as telephone books, public websites, business cards, university listings, etc. This PII includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. This category of PII will be referred to as Public PII and must be protected with at least NIST SP 800-53 low level controls.

- **Protected Personally Identifiable Information**

SC also recognizes there is another category of PII that requires enhanced protection, which will be referred to as Protected PII. This typically includes information which, if compromised, can cause serious or severe harm to an individual (such as identity theft). Protected PII is defined as:

> *An individual's first name or first initial and last name in combination with any one or more of the following data elements types of information including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts, etc. requires enhanced protection.*

Protected PII must be protected with at least NIST SP 800-53 moderate level controls. When Public PII is combined with Protected PII, then the combined information must also be protected with at least NIST SP 800-53 moderate level controls.

Policy

- ### **General**

  All electronic copies of Protected PII will reside within an accreditation boundary protected at least at the moderate level. Protected PII is not to be downloaded to mobile devices (such as laptops, Personal Digital Assistants (PDAs), or removable media, or to systems outside the protection of the accreditation boundary).

- ### **Waiver**

  If there is an operational or business need to store Protected PII outside the accreditation boundary (in particular on laptops and mobile devices), a waiver may be granted by the Designated Approving Authority (DAA). In instances where a waiver has been granted, the controls as specified by DOE CIO CS-38 will be applied. In particular, encryption (FIPS 140-2 compliant) will be used to protect PII and a 90-day review policy will be enforced.

- ### **Remote Access**

  If there is an operational or business need to access Protected PII data from outside the accreditation boundary, an automatic disconnect after 30 minutes of inactivity will be enforced. In addition, two-factor authentication will be required to access Protected PII.

- ### **Incident Reporting**

  Within 45 minutes after discovery of a real or suspected loss of Protected PII data, Computer Incident Advisory Capability (CIAC) needs to be notified (ciac@ciac.org).

Reporting of incidents involving Public PII will be in accordance with normal incident reporting procedures.

5.1.3.4 SC Policy on CS-05, Interconnect Agreement Guidance

OMB Circular A-130 states that written management authorization (often in the form of a Memorandum of Understanding or Agreement (MOU/MOA)) must be obtained prior to connecting with other systems and/or sharing sensitive data/information. Interconnection agreements must be analyzed and documented according to the guidance provided in NIST 800-47, "*The Security Guide for Interconnecting Information Technology Systems*". NIST Special Publication 800-47 provides guidance for planning, establishing, maintaining and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.

Laboratory and Site Office managers will provide written authorization describing any system vulnerability and will detail the rules of behavior and controls that must be maintained by the interconnecting systems. As a matter of SC policy, SC Federal and SC contractor cyber enclaves would need to specifically address the risks for having enclaves co-mingled.

An MOU/MOA is required when a trust relationship exists between non-research information processing systems on disparate networks. The MOU/MOA is a written agreement of cooperation between organizations defining the roles and responsibilities of each organization in relation to the other with respect to security issues over which the organizations have concurrent jurisdiction. The purpose of the MOU/MOA is to assure that the security posture of either organization is not degraded by changes to the security controls implemented for either network. An example of an acceptable MOU/MOA template that organizations may use to assure that this trust relationship is maintained properly is provided below.

MEMORANDUM OF UNDERSTANDING

Between

(Name of Science Site)

and

(Name of User Site)

This Memorandum of Understanding (MOU) between (Science Site) and the (User Site), Designated Approving Authority for (Company Name), is for the purpose of establishing a trusted communications link between (Science Site) and the (User Site) for the electronic transfer of information. Each of the undersigned agrees to and understands the procedures that will be in effect and adhered to. It is also understood that this MOU summarizes the information system (IS) security requirements for approval purposes, and supplements (Science Site) and the (User Site) approved system security plan (SSP).

1. Contract Information

This MOU describes the network arrangement between (Science Site) and the (User Site), in support of the (Name of Program). The (Name of Program) is a (brief description of program) sponsored by (DOE Agency). The contract number is (Contract Number). The prime contractor is (Name of Prime Contractor).

The following key points of contact are identified:

(SCIENCE SITE)

NAME	TITLE	PHONE
	Manager of Security	
	Program Manager	
	Program Security Supervisor	
	Information Systems Security Manager (ISSM)	

(USER SITE)

NAME	TITLE	PHONE
	Manager of Security	
	Program Manager	
	Program Security Supervisor	
	Information Systems Security Manager (ISSM)	

At (Science Site) direction, (User Site) is establishing an access capability to the (Name of Computer System,) access site is located at (User site or Company, as appropriate). *(Note to Template User: Please word this paragraph so that it is obvious who will be the host, if applicable, and who will be the remote computer system).* This capability will allow (Science User sites) personnel to access the (Name of information systems) as remote users. The (User Agency) is located at (address.)

2. Description

(Science site) operates the (Name of System) at (insert level of control – low, moderate, high), whereby all users have the need to know for all information on the system.

(Describe connection. An example follows): The (User site) will be connected to the (Name of System) at (Science site location), by a (insert specifics) communications circuit for the transfer of data via a (describe type of network). The circuit will be protected at each end by (describe protection mechanism/device that provides the required level of security).

3. System Security Officer (or appropriate title) Responsibilities

The System Security Officer at (Science Site) will have the following responsibilities. He or she will brief operator personnel involved with use of communications and network operating procedures and their responsibilities for safeguarding information in accordance with the requirements of the CSPP. The Information System (IS) Security Officer at (User Agency Site) will conduct an equivalent briefing for information system responsible personnel.

These briefings will include:

a. The need for sound security practices for protecting information handled by their respective Information System, including all input, storage, and output products.

b. The specific security requirements associated with their respective IS as they relate to CSPP controls and operator access requirements.

c. The security reporting requirements and procedures in the event of a system malfunction or other security incident.

d. What constitutes an unauthorized action as it relates to system usage?

e. Their responsibility to report any known or suspected security violations.

It is the responsibility of each individual operator to understand and comply with all required procedures for using the systems at each site, as described in their respective system security plans.

4. Approval

The communication link between (Science Site) and (User Site) shall not be initialized until approval of these procedures by the DAA is indicated below.

(Science Site)	(User Agency)
______________________________	______________________________
(Name of DAA)	(Name of User Agency Official and Rank)
Title:	Title:
Designated Approving Authority	Designated Approving Authority

Optional Signatures

(Science Site)	(User Site)
______________________________	______________________________
(Name of Security Official)	(Name of Security Official)
Title	Title

(Name of Company)

____

Name of Facility Security Officer
Facility Security Officer

6.0 References

The following summarizes high-level references relevant to this management system.

OMB Circular A-123, Management Accountability and Control, (August 4, 1986), revised (December 21, 2004)

OMB Circular A-130 Appendix III, Security of Federal Automated Information Resources, (November 2003)

OMB Memorandum M-96-20, Implementation of the Information Technology Management Reform Act of 1996, (April 4, 1996)

OMB Memorandum M-97-02, Funding Information Systems Investments, (October 25, 1996)

OMB Memorandum M-99-05, Instructions for Complying With the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records", (January 7, 1990)

OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, (June 2, 1999)

OMB Memorandum M-99-20, Security of Federal Automated Information Resources, (June 23, 1999)

OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, (February 28, 2000)

OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, (April 25, 2000)

OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, (June 22, 2000)

OMB Memorandum M-00-015, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, (September 25, 2000)

OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, (January 16, 2001)

OMB Memorandum M-01-26, Component-Level Audits, (July 10, 2001)

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (September 30, 2003)

OMB Memorandum M-04-04, E-Authentication Guidance, (December 16, 2003)

OMB Memorandum M-04-25, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, (July 17, 2006)

OMB Memorandum M-04-26, Personal Use Policies and "File Sharing" Technology, (September 8, 2004)

OMB Memorandum M-05-02, Financial Management Systems, (December 1, 2004)

OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, (December 17, 2004)

OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, (February 11, 2005)

OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, (May 22, 2006)

OMB Memorandum M-06-16, Protection of Sensitive Agency Information, (June 23, 2006)

OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments", (July 12, 2006)

NIST Federal Information Processing Standard (FIPS) 201-1, National Institute of Standards and Technology (NIST), Personal Identity Verification (PIV) of Federal Employees and Contractors, (March 2006)

NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006)

NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, (February 2004)

NIST FIPS 142-2, Security requirements for Cryptographic Modules, (May 2001)

NIST Special Publication (SP) 800-92, Guide to Computer Security Log Management, (September 2006)

NIST SP 800-88, Guidelines for Media Sanitization, (September 2006)

NIST SP 800-83, Guide to Malware Incident Prevention and Handling. (November 2005)

NIST SP 800-73, Rev. 1, Interfaces for Personal Identity Verification, March 2006 (updated April 20, 2006)

NIST SP 800-70, The NIST Security Configuration Checklists Program, (May 2005)

NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process, (January 2005)

NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Revision 1, (June 2004)

NIST SP 800-61, Computer Security Incident Handling Guide, (January 2004)

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, (June 2004)

NIST SP 800-55, Security Metrics Guide for Information Technology Systems, (July 2003)

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, (April 2006)

NIST SP 800-53, Rev. 1, Recommended Security Controls for Federal Information Systems, (December 2006)

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program (October 2003)

NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, (November 2002)

NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, (August 2002)

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, (May 2004)

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, (June 2002)

NIST SP 800-30, Risk Management Guide for Information Technology Systems, (July 2002)

NIST SP 800-26, Rev. 1, Guide for Information Security Program Assessments and System Reporting Form, (November 2001)

NIST SP 800-18, Rev. 1, Guide for Developing Security Plans for Federal Information Systems, (February 2006)

DOE Chief Information Officer Guidance – Cyber Security

CS-01, Controls for Unclassified Systems, (June 30, 2006)

CS-01, Management, Operational and Technical Controls Guidance, (July 6, 2006)

CS-02, Certification and Accreditation, (March 24, 2006)

CS-03, Risk Management, (June 30, 2006)

CS-04, Vulnerability Management, (July 31, 2006)

CS-05, Interconnect Agreements, (July 31, 2006)

CS-06, Plans of Actions and Milestones (POA&M), (September 07, 2006)

CS-07, Contingency Planning, (August 26, 2006)

CS-08, Configuration Management, (November 27, 2006)

CS-09, Incident Management, (January 2007)

CS-11, Clearing and Media Sanitization (January 2007)

CS-12, Password Management, (June 30, 2006)

CS-13, Wireless Devices and Information Systems, (June 30, 2006)

CS-14, Portable/Mobile Devices, (January 2007)

CS-15, Personally Owned Devices, (January 2007)

CS-18, Foreign National Access to DOE Information Systems, (January 2007)

CS-20, INFOCON, (December 06, 2006)

CS-23, Peer-To Peer Networking, (December 2006)

CS-24, Remote Access, (January 2007)

CS-37, Security, Testing and Evaluation, (January 2007)

CS-38A, Protection of Sensitive Unclassified Information, including Personally Identifiable Information, (November 2006)